W

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/740,484	12/22/2003	Makan Pourzandi	P18829US1	2065

7590 04/03/2007

ALEX NICOLAESCU
Ericsson Canada Inc.
Patent Department (LMC/M/P)
8400 Decarie Blvd.
Town Mount Royal, QC H4P 2N2
CANADA

EXAMINER	
ZEE, EDWARD	
ART UNIT	**PAPER NUMBER**
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/03/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/740,484	**Applicant(s)** POURZANDI ET AL.	
	Examiner Edward Zee	**Art Unit** 2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *22 December 2003* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *05/04/05*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the original filing of December 22, 2003. Claims 1-38 are pending and have been considered below.

Drawings

2. The informal drawings are not of sufficient quality to permit examination. Accordingly, replacement drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to this Office action. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action.

Applicant is given a TWO MONTH time period to submit new drawings in compliance with 37 CFR 1.81. Extensions of time may be obtained under the provisions of 37 CFR 1.136(a). Failure to timely submit replacement drawing sheets will result in ABANDONMENT of the application.

3. New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because the drawings are hand drawn. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Specification

4. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

5. The abstract of the disclosure is objected to because it contains more than 150 words.

Correction is required. See MPEP § 608.01(b).

6. The disclosure is objected to because of the following informalities: the examiner notes spelling errors and the use of the acronyms (ie. RSA, etc.) throughout the specification without first including a description in plain text, as required.

Appropriate correction is required.

Claim Objections

7. Claim 21 is objected to because of the following informalities: it appears that claim 21 is a dependent claim of claim 20, however no dependency has been specified in the preamble. The examiner will note this when considering the claim below.

Appropriate correction is required.

Claim Rejections - 35 USC § 101

8. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 20-38 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. These claims are drawn to a computer program per se. A computer program is not a series of steps or acts and this is not a process. A computer program is not a physical article or object and as such is not a machine or manufacture. A computer program is not a combination of substances and there for is not a compilation of matter. Thus, a computer program by itself does not fall within any of the four categories of invention. Therefore, claims 20-38 are not statutory.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1, 2, 6, 10, 20, 21, 25 and 29 are rejected under 35 U.S.C. 102(e) as being anticipated by Rose et al. (2004/0039908).

Claims 1 and 20: Rose et al. discloses a method and software application for digital signature of an electronic file comprising the steps of:

a. determining*(computing)* a portion of the electronic file*(block)* that is to used for computing a digital signature*(encrypt)* [page 7, paragraph 0094-0095];

b. digitally signing*(encrypting)* a block of data that consists of the determined*(computed)* portion and creating the digital signature of the electronic file*(encrypted data)* [page 7, paragraph 0094-0095];

c. wherein the portion of the electronic file that is to be used for the digital signature is computed using one or more functions that are known to a signer of the electronic file who executes the digital signature [page 7, paragraph 0094-0095].

Claims 2 and 21: Rose et al. discloses a method and software application as in claims 1 and 20 above and further discloses:

a. computing a Message Digest (MD) value using the determined portion of the electronic file [page 3, paragraph 0036];

b. wherein the block of data that is digitally signed in consists of the MD value [page 3, paragraph 0036].

Claims 6 and 25: Rose et al. discloses a method and application software as in claims 2 and 21 above and further discloses appending the digital signature to the electronic file and creating a digitally signed electronic file*(the MAC tag is then appended to the message)* [page 6, paragraph 0076].

Claims 10 and 29: Rose et al. discloses a method and software application for digital signature verification of an electronic file comprising the steps of:

a. extracting the digital signature from the electronic file and determining a portion of the electronic file that was used for computing the digital signature*(generate intermediate ciphertext blocks from the received transmission blocks)* [page 7, paragraph 0100-0101];

b. decrypting the digital signature using a public key of the signer of the electronic file, and obtaining a block of data and comparing the portion of the electronic file that was used for computing the digital signature with the block of data for determining an authenticity and an integrity of the electronic file*(performs verification of digital signature using public key)* [page 3, paragraph 0035 and page 7, paragraph 0103];

e. wherein the portion of the electronic file that was used for computing the digital signature is computed using one or more functions that are known to a verifier of the digital signature verification of the electronic file [page 7, paragraphs 0094-0095].

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 3-5, 12-14, 22-24 and 31-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rose et al. (2004/0039908) in view of Okano (6,839,844).

Claims 3 and 22: Rose et al. discloses a method and software application as in claims 2 and 21 above and further discloses dividing the electronic file*(message)* into a plurality of blocks*(message blocks)* [page 5, paragraph 0070], but does not explicitly disclose that:

a. from each block of the plurality of blocks, extracting a block portion and copying the block portion into a buffer;

b. wherein when the block portion is extracted and copied into the buffer for each block of the plurality of blocks, the buffer comprises the portion of the electronic file that is to be digitally signed.

However, Okano discloses a similar method and software application and further discloses:

a. from each block of the plurality of blocks, extracting a block portion and copying the block portion into a buffer*(save the selected portion in a separate file)* [column 3, lines 33-37];

b. wherein when the block portion is extracted and copied into the buffer for each block of the plurality of blocks, the buffer comprises the portion of the electronic file that is to be digitally signed*(encrypt file)* [column 3, lines 33-37].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to copy the block portion disclosed by Rose et al. into a buffer before digitally signing the blocks. One would have been motivated to do so in order to increase system performance by using a separate module to perform the encryption process.

Claims 4 and 23: Rose et al. and Okano disclose a method and software application as in claims 3 and 22 above and Rose et al. further discloses that for each block of the plurality of blocks, computing a value m using the one or more functions and within a block of the plurality of blocks*(calculate value $E_{k1}(r+i)$ which is used to encrypt only the bits that are transmitted in encrypted form)*, at a location m bytes apart from a beginning of the block, extracting the block portion and copying the block portion into the buffer, wherein the block portion has p bytes of length [page 7, paragraphs 0094-0095].

Claims 5 and 24: Rose et al. and Okano disclose a method and software application as in claims 4 and 23 above and Rose et al. further discloses that for computing the value of m, a first function*(compute $E_{k1}(r+i)$)* is applied on a shared secret key*(k1)* of the signer of the electronic file, and wherein a second function is applied on a result of the first function and on a variable j that represents the number of a current block from the plurality of blocks of the electronic file*(the bit-wise AND function applied to: M_i AND $E_{k1}(r+i)$)* [page 7, paragraphs 0094-0095].

Claims 12 and 31: Rose et al. discloses a method and software application as in claims 11 and 30 ~~above~~ below and further discloses dividing the electronic file*(message)* into a plurality of blocks*(message blocks)* [page 5, paragraph 0070], but does not explicitly disclose that:

a. from each block of the plurality of blocks, extracting a block portion and copying the block portion into a buffer;

b. wherein when the block portion is extracted and copied into the buffer for each block of the plurality of blocks, the buffer comprises the portion of the electronic file that was used for computing the digital signature.

However, Okano discloses a similar method and software application and further discloses:

a. from each block of the plurality of blocks, extracting a block portion and copying the block portion into a buffer wherein when the block portion is extracted and copied into the buffer for each block of the plurality of blocks, the buffer comprises the portion of the electronic file that was used for computing the digital signature*(extracting the encrypted portions to a decryptor for decrypting)* [column 3, lines 38-42].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to copy the block portion disclosed by Rose et al. into a buffer before decrypting the blocks. One would have been motivated to do so in order to increase system performance by using a separate module to perform the decryption process.

Claims 13 and 32: Rose et al. and Okano disclose a method and software application as in claims 12 and 31 above and Rose et al. further discloses that for each block of the plurality of blocks, computing a value m using the one or more functions and within a block of the plurality of blocks*(calculate value $E_{k1}(r+i)$ which is used to generate the intermediate cipherblocks for decrypting)*, at a location m bytes apart from a beginning of the block, extracting the block portion and copying the block portion into the buffer, wherein the block portion has p bytes of length [page 7, paragraphs 0094, 0095 and 0100].

Claims 14 and 33: Rose et al. and Okano disclose a method and software application as in claims 13 and 32 above and Rose et al. further discloses that for computing the value of m, a first function*(compute $E_{k1}(r+i)$)* is applied on a shared secret key*(k1)* of the signer of the electronic file, and wherein a second function is applied on a result of the first function and on a variable j that represents the number of a current block from the plurality of blocks of the electronic file*(the bit-wise AND function applied to: M_i AND $E_{k1}(r+i)$)* [page 7, paragraphs 0094-0095].

13. Claims 7-9, 11, 15-19, 26-28, 30 and 34-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rose et al. (2004/0039908).

Claims 7-9, 26, 27 and 28: Rose et al. discloses a method and software application as in claims 2 and 21 above, but does not explicitly disclose that the electronic file is a binary, executable and shared library file. However, it would have been obvious to one of ordinary skill in the art at the time of invention that the electronic file can be a binary file, executable file, shared library file or any other form of electronic data. One would have been motivated to do so in order to make the system more versatile by being able to accommodate all types of data format.

Claims 11 and 30: Rose et al. discloses a method and software application as in claims 10 and 29 above and further discloses using a message digest to compute the digital signature [page 3, paragraph 0036], but does not explicitly disclose:

a. computing a Message Digest (MD2) value using the determined portion of the electronic file;

b. wherein the said block of data obtained comprises an MD1 value [page 3, paragraph 0036];

c. comparing the MD1 value with the MD2 value.

However, it would have been obvious to one of ordinary skill in the art at the time of invention that the block of data obtained after decrypting the signature, which is a digital signature of a message digest, will be a message digest. One would be motivated to perform the encryption/decryption scheme in this manner in order to retain a conventional asymmetric authentication system, which will insure more predictable results. Furthermore, it would have been obvious to one of ordinary skill in the art at the time of invention to compute the Message Digest MD2 and compare it to MD1. One would have been motivated to do so in order to verify that the data has not been compromised during transmittal.

Claims 15-17, 34, 35 and 36: Rose et al. discloses a method and software application as in claims 11 and 30 above, but does not explicitly disclose that the electronic file is a binary, executable and shared library file. However, it would have been obvious to one of ordinary skill in the art at the time of invention that the electronic file can be a binary file, executable file, shared library file or any other form of electronic data. One would have been motivated to do so in order to make the system more versatile by being able to accommodate all types of data format.

Claims 18 and 37: Rose et al. discloses a method and software application as in claims 11 and 30 above, but does not explicitly disclose that if the MD1 value is equal to the MD2 value, it is concluded that the digital signature is valid and the electronic file is authentic and unmodified with respect to the electronic file that was digitally signed. However, it would have been obvious to one of ordinary skill in the art at the time of invention that if MD1 and MD2 match, one can conclude that the digital signature is valid and the electronic file is authentic. One would be motivated to perform the encryption/decryption scheme in this manner in order to retain a conventional asymmetric authentication system, which will insure more predictable results.

Claims 19 and 38: Rose et al. discloses a method and software application as in claims 11 and 30 above, but does not explicitly disclose that if MD1 value is not equal to MD2 value, it is concluded that the digital signature is invalid and that the electronic file is corrupted. However, it would have been obvious to one of ordinary skill in the art at the time of invention that if MD1 and MD2 do not match, one can conclude that the digital signature is invalid and the electronic file is corrupted. One would be motivated to perform the encryption/decryption scheme in this manner in order to retain a conventional asymmetric authentication system, which will insure more predictable results.

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Roberts (5,008,935) and Hawkes et al. (2004/0019782).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edward Zee whose telephone number is (571) 270-1686. The examiner can normally be reached on Monday through Thursday 6:30AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James W. Myhre can be reached on (571) 270-1065. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ
March 28, 2007

James W. Myhre
Supervisory Patent Examiner

***